April 24, 2006

Information Technology Management

Review of the Information Security Operational Controls of the Defense Logistics Agency's Business Systems Modernization-Energy
(D-2006-079)

Department of Defense
Office of Inspector General

Quality *Integrity* *Accountability*

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
24 APR 2006		**00-00-2006 to 00-00-2006**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Information Technology Management: Review of the Information Security Operational Controls of the Defense Logistics Agency's Business Systems Modernization-Energy	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **ODIG-AUD (ATTN: AFTS Audit Suggestions),Inspector General of the Department of Defense,400 Army Navy Drive (Room 801),Arlington,VA,22202-4704**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**49**	

Additional Copies

To obtain additional copies of this report, visit the Web site of the Department of Defense Inspector General at http://www.dodig.mil/audit/reports or contact the Secondary Reports Distribution Unit, Audit Followup and Technical Support at (703) 604-8937 (DSN 664-8937) or fax (703) 604-8932.

Suggestions for Future Audits

To suggest ideas for or to request future audits, contact Audit Followup and Technical Support at (703) 604-8940 (DSN 664-8940) or fax (703) 604-8932. Ideas and requests can also be mailed to:

ODIG-AUD (ATTN: AFTS Audit Suggestions)
Department of Defense Inspector General
400 Army Navy Drive (Room 801)
Arlington, VA 22202-4704

Acronyms

ATO	Authority To Operate
BSM-E	Business Systems Modernization-Energy
C&A	Certification and Accreditation
CIO	Chief Information Officer
COOP	Continuity Of Operations Plan
DESC	Defense Energy Support Center
DLA	Defense Logistics Agency
DAA	Designated Approving Authority
EDC	Enterprise Data Center
FISMA	Federal Information Security Management Act
FAS	Fuels Automated System
FES	Fuels Enterprise Server
IA	Information Assurance
IT	Information Technology
IATO	Interim Authority To Operate
MOU/A	Memorandum Of Understanding/Agreement
MAC	Mission Assurance Category
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
POA&M	Plan Of Action and Milestones
SSAA	System Security Authorization Agreement

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON, VIRGINIA 22202-4704

April 24, 2006

MEMORANDUM FOR DIRECTOR, DEFENSE LOGISTICS AGENCY

SUBJECT: Report on Review of the Information Security Operational Controls of the Defense Logistics Agency's Business Systems Modernization-Energy (Report No. D-2006-079)

We are providing this report for review and comment. We considered comments from the Defense Logistics Agency when preparing the final report.

DoD Directive 7650.3 requires that all recommendations be resolved promptly. The Defense Logistics Agency comments were partially responsive to two recommendations and not responsive to fourteen recommendations. All recommendations remain unresolved. Therefore, we request that the Defense Logistics Agency Chief Information Officer/Designated Approving Authority reconsider her position and provide additional comments on all Recommendations by May 24, 2006.

If possible, please send management comments in electronic format (Adobe Acrobat file only) to AudROS@dodig.mil. Copies of the management comments must contain the actual signature of the authorizing official. We cannot accept the / Signed / symbol in place of the actual signature. If you arrange to send classified comments electronically, they must be sent over the SECRET Internet Protocol Router Network (SIPRNET).

We appreciate the courtesies extended to the staff. Questions should be directed to Ms. Kathryn M. Truex at (703) 604-8966 (DSN 664-8966) or Ms. Sarah A. Davis at (703) 604-9031 (DSN 664-9031). See Appendix D for the report distribution. The team members are listed inside the back cover.

By direction of the Deputy Inspector General for Auditing:

Wanda A. Scott
Assistant Inspector General
Readiness and Operations Support

Department of Defense Office of Inspector General

Report No. D-2006-079 **April 24, 2006**
(Project No. D2005-D000AL-0158.000)

Review of the Information Security Operational Controls of the Defense Logistics Agency's Business Systems Modernization-Energy

Executive Summary

Who Should Read This Report and Why? The DoD Chief Information Officer; Director, Defense Logistics Agency; Defense Logistics Agency Chief Information Officer; and Chief Information Officers of the Air Force, Army, and Naval branches of the military should read this report to obtain information about Business Systems Modernization-Energy (Fuels Automated System). This report discusses how Business Systems Modernization-Energy (Fuels Automated System) is managed and controlled by the Defense Logistics Agency and how it is used at the base level by the Military Services.

Background. This report was prepared in response to the annual reporting requirements of the Federal Information Security Management Act of 2002. The Federal Information Security Management Act of 2002 is title III, section 301 of the E-Government Act of 2002 (Public Law 107-347). The Federal Information Security Management Act provides a comprehensive framework for ensuring the effectiveness of information security controls, management, and oversight required to protect Federal information and information systems. In addition, the Federal Information Security Management Act requires the Inspectors General of each agency to perform an independent evaluation of the agency's information security programs and practices.

The Defense Logistics Agency supplies the nation's Military Services and several civilian agencies with the critical resources they need to accomplish their worldwide missions. The Defense Energy Support Center is the component of DLA assigned responsibility for providing the DoD and other government agencies with comprehensive energy solutions. The Business Systems Modernization-Energy (Fuels Automated System) supports the Defense Energy Support Center and the Military Services in performing their responsibilities in fuel management and distribution. The information security operational controls related to the Business Systems Modernization-Energy (Fuels Automated System) should operate effectively and provide an appropriate level of information assurance.

Results. The DLA Chief Information Officer has not fully implemented information security operational controls at the Defense Logistics Agency. Specifically, the Defense Logistics Agency Chief Information Officer did not:

- ensure that Business Systems Modernization-Energy (Fuels Automated System) was fully certified and accredited;

- address all system security weaknesses in the plans of action and milestones;
- ensure that adequate user access controls were in place;
- consistently provide users with annual security awareness training; and
- complete and test system-wide continuity of operations plans.

In addition, weaknesses were found in the Defense Logistics Agency Management Control Program for the Business Systems Modernization-Energy (Fuels Automated System) certification and accreditation, user access controls, training requirements, and continuity of operations plan. As a result, the Business Systems Modernization-Energy (Fuels Automated System) operated with vulnerabilities that present potential risks to the Defense Logistics Agency and the DoD. See the Finding section of the report for the detailed recommendations.

Management Comments and Audit Response. The Defense Logistics Agency Chief Information Officer/Designated Approving Authority nonconcurred with twelve of the recommendations and concurred with comments on four recommendations. The comments stated that the Business Systems Modernization-Energy (Fuels Automated System) Base Level Support Application Type Accreditation was developed in accordance with DoD 8510.1-Manual, "DoD IT and Security Certification and Accreditation Process Application Manual," July 31, 2000, which designates Base Level personnel as the responsible source for complying with information assurance responsibilities. The comments repeatedly stated that the Defense Logistics Agency is not responsible for Base Level compliance with information assurance guidance. The comments also state that the established Defense Logistics Agency One Book chapters fully address the policies required to implement and sustain an effective information assurance program. Additionally, the comments state that updates to the Business Systems Modernization-Energy (Fuels Automated System) will occur once the system migrates to the Enterprise Data Center. Furthermore, the comments state that the provisions within the Business Systems Modernization-Energy (Fuels Automated System) Base Level Support Application System Security Authorization Agreement are binding to all organizations where the application is installed and operated.

The Defense Logistics Agency Chief Information Officer/Designated Approving Authority comments were nonresponsive to fourteen recommendations and partially responsive to two recommendations. The Defense Logistics Agency comments contained inaccurate dates and incorrect citations of DoD policy. The Defense Logistics Agency is required to develop a plan of action and milestones for all programs and systems where an information security weakness has been identified. The Business Systems Modernization-Energy (Fuels Automated System) Base Level Support Application System Security Authorization Agreement should have included a statement that defines the intended operating environment as well as any operating procedures required for the type accredited system. In addition, the program manager, user representative, and information system security officer should have ensured that proper security operating procedures, configuration guidance, and training was delivered with the system. See the Finding section of the report for a discussion of management comments and the Management Comments section of the report for the complete text of the comments.

Table of Contents

Background

Defense Logistics Agency. The Defense Logistics Agency (DLA) supplies the nation's military services and several civilian agencies with the critical resources they need to accomplish their worldwide missions. DLA provides wide-ranging logistics support for peacetime and wartime operations, as well as emergency preparedness and humanitarian missions. The Defense Energy Support Center (DESC) is the component of DLA assigned responsibility for providing the DoD and other government agencies with comprehensive energy solutions in the most effective and economical manner possible. The basic mission of DESC is to support the warfighter and manage the energy sources of the future.

Business Systems Modernization-Energy (Fuels Automated System) Background. The Business Systems Modernization-Energy (BSM-E) (formerly the Fuels Automated System (FAS)) is categorized by the DLA as a Mission Assurance Category (MAC) II[1] and is responsible for managing all DoD fuels. BSM-E (FAS) supports the DESC and the Military Services in performing their responsibilities in fuel management and distribution. The BSM-E (FAS) is considered a multi-functional automated information system that provides point of sale data collection, inventory control, finance and accounting, procurement, and facilities management. The BSM-E (FAS) provides an advanced tool for DESC's worldwide energy support mission, with five primary software programs:

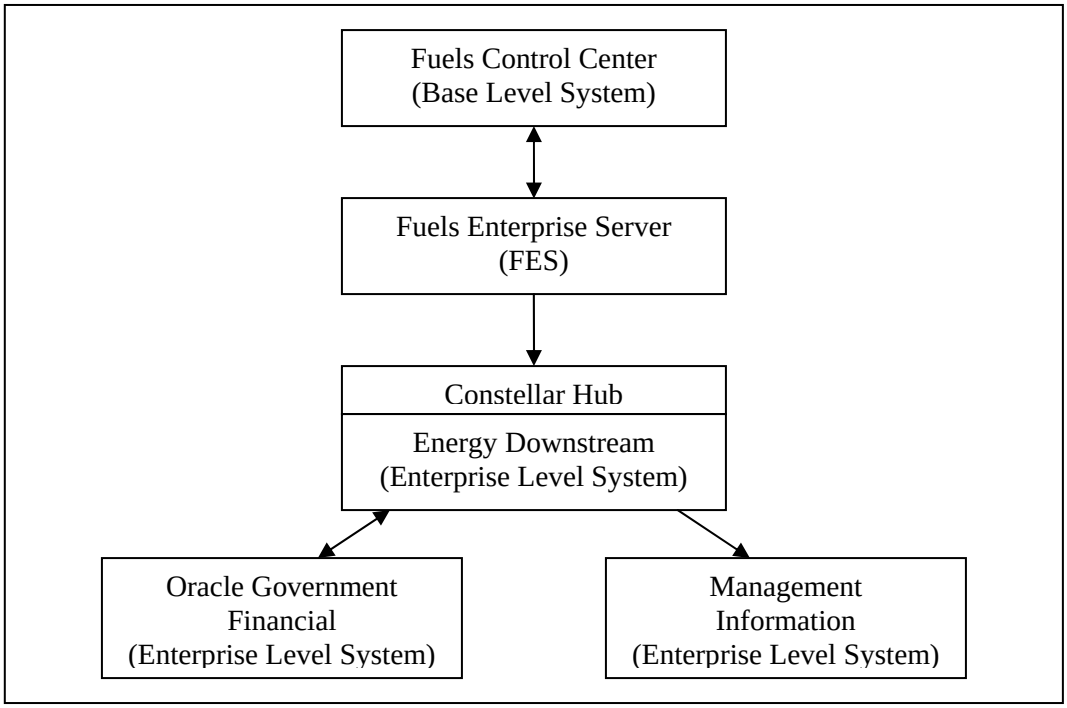
- Fuels Control Center;
- Fuels Enterprise Server (FES);
- Energy Downstream;
- Oracle Government Financial; and
- Management Information.

The BSM-E (FAS) is comprised of a Base Level system, the FES, and an Enterprise Level system. The BSM-E (FAS) Base Level system consists of computers loaded with Fuels Control Center software. The Base Level system provides the capability to order fuel from existing contracts; document receipt of fuel; document issues/sales; compare booking to physical inventory accounting; and schedule quality checks and physical plant inspections. The FES is the single point of entry for base level transactions. The FES receives, sorts, validates, and manages data entered from the Base Level system and sends that data to the Enterprise Level system. The Enterprise Level system consists of Energy Downstream software, Oracle Government Financial software, Management

[1] Mission Assurance Category II (MAC II) systems handle information that is important to the support of deployed and contingency forces. The consequences of loss of availability could include delay or cause degradation in providing important support services or commodities that may seriously impact mission effectiveness or operational readiness. MAC II systems require additional safeguards beyond best practices to ensure assurance.

Information software, and the Constellar Hub (serving as a gateway from FES to Energy Downstream).

The BSM-E (FAS) is supported at three military locations: the Defense Supply Center Richmond in Richmond, Virginia; the DLA Headquarters in Fort Belvoir, Virginia; and the Washington Navy Yard in Washington, D.C. The Defense Supply Center Richmond houses the primary production equipment, while the Washington Navy Yard/DLA hosts the alternate, test, development, and control systems and provides Continuity of Operations capability. The figure below shows the BSM-E (FAS) data flow process.



BSM-E (FAS) Data Flow Process

Government Accountability Office Report 06-31. In October 2005, the Government Accountability Office issued a DLA Information Security Report stating that DLA had not fully implemented an agency-wide information security program to protect the information and information systems that support its operations and assets. Specifically, the Government Accountability Office stated that DLA did not consistently assess risks for its information systems; sufficiently train employees who have significant information security responsibilities or adequately complete training plans; annually test and evaluate the effectiveness of management and operational security controls; or sufficiently complete plans of action and milestones for mitigating known information security deficiencies.

Objectives

The overall objective of the audit was to determine whether information security operational controls operate effectively and provide an appropriate level of information assurance. Specifically, during this audit we assessed the adequacy and effectiveness of the security program; the implementation and effectiveness of access controls; and the procedures and testing of contingency and continuity of operations plans. We also reviewed the Management Control Program as it related to the overall objective. See Appendix A for a discussion of audit scope and methodology. See Appendix B for prior audit coverage related to the overall objective. See Appendix C for information security operational controls criteria.

Management Control Program Review

DoD Directive 5010.38, "Management Control Program," August 16, 1996, and DoD Instruction 5010.40, "Management Control Program Procedures," August 18, 1996, require DoD organizations to implement a comprehensive system of management controls that provides reasonable assurance that programs are operating as intended and to evaluate the adequacy of the controls.

Scope of the Review of the Management Control Program. The audit team examined the DLA Management Control Program by following the procedures the audit team outlined to achieve their objective. The objective was to determine whether information security operational controls operate effectively and provide an appropriate level of information assurance. The audit team tested the DLA Management Control Program by reviewing the certification and accreditation (C&A) of the system, the security program, access controls, and contingency and continuity of operations plans (COOP). In addition, management's self-evaluation of the applicable management controls was examined.

Adequacy of Management Controls. The audit team found weaknesses in the DLA Management Control Program for the BSM-E (FAS) C&A, user access controls, training requirements, and COOP. Specific results are in the Finding section of the report. The implementation of the report recommendations will correct the identified weaknesses. A copy of the final report will be provided to the senior official responsible for management controls at DLA.

Adequacy of Management's Self-Evaluation. The audit team found weaknesses with the review of the Management Control Program performed by DLA. DLA conducted a review of the J6F[2] system of internal accounting and administrative control. The DLA review of the integrity of the J6F information systems did not recognize the risks that DLA systems face in regards to logon identities and passwords, user access, and training requirements when operated at non-DLA locations.

[2] J6 is the Information Operations organization of DLA. J6F is the Information Operations Directorate, Fort Belvoir site.

Implementation of Security Operational Controls for the BSM-E (FAS) System

The DLA Chief Information Officer (CIO) has not fully implemented information security operational controls at the DLA. Specifically, the DLA CIO did not:

- ensure that BSM-E (FAS) was fully certified and accredited;
- address all system security weaknesses in the plans of action and milestones (POA&Ms);
- ensure that adequate user access controls were in place;
- consistently provide users with annual security awareness training; and
- complete and test system-wide continuity of operations plans.

This occurred because DLA did not adequately assign Information Assurance (IA) responsibilities and have an effective Management Control Program for IA. As a result, BSM-E (FAS) operated with vulnerabilities that present potential risks to the DLA and the DoD.

Federal Information Security Management Act

The E-Government Act of 2002 (Public Law 107-347), title III, section 301, "Federal Information Security Management Act of 2002," provides a comprehensive framework for ensuring the effectiveness of information security controls, management, and oversight required to protect Federal information and information systems. The Federal Information Security Management Act (FISMA) requires Federal agencies to develop, document, and implement an agency-wide information security program and annually report to the Office of Management and Budget (OMB) and the Congress the adequacy and effectiveness of information security policies, procedures, and practices. FISMA requires each agency to perform annual testing and evaluation of the management, operational, and technical controls and also states that each agency's security program shall include the provision for the continuity of operations for information systems that support the operations and assets of the agency. In addition, the FISMA requires the Inspectors General of each agency to perform an independent evaluation of the agency's information security programs and practices.

As mandated by FISMA, Section 20 of the National Institute of Standards and Technology (NIST) Act (15 U.S.C. 278g-3), was amended to insert that NIST had the mission of developing standards, guidelines, and associated methods and techniques for information systems. This includes minimum requirements for information systems used or operated by an agency or by a contractor of an

agency or other organization on behalf of an agency, other than national security systems. NIST was also assigned responsibility for developing standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets, but such standards and guidelines would not apply to national security systems.

BSM-E (FAS) Security Operational Controls

The DLA CIO did not fully implement information security operational controls. According to the DLA One Book Policy, "IA Operational Controls," August 19, 2004, the implementation of IA operational controls is necessary to ensure the confidentiality, integrity, and availability of Sensitive but Unclassified and classified data processed and stored by information technology (IT) systems in a day-to-day operational environment.

Certification and Accreditation. DLA had not fully certified and accredited the BSM-E (FAS) since 2001. In October 2003, the DLA Designated Approving Authority (DAA) formally designated the BSM-E (FAS) as a MAC II Sensitive System in accordance with DoD Instruction 8500.2. Additionally, the DAA required that the BSM-E (FAS) System Security Authorization Agreement (SSAA) be updated and completed by December 30, 2003. On July 1, 2004, the DAA granted BSM-E (FAS) an Interim Authority to Operate (IATO) for 180 days to accomplish IA remediation actions identified in the POA&M. DLA completed a new BSM-E (FAS) SSAA in October 2004; however, the DAA did not issue another IATO until December 30, 2004, because an Authority to Operate (ATO) could not be granted based on outstanding POA&M items. The Memorandum from the DLA DAA stated that the IATO expired on June 28, 2005, which should have been sufficient time for J6F to resolve the existing vulnerabilities and submit the necessary documentation to support an ATO.

On May 13, 2005, the DAA for BSM-E (FAS) issued an IATO Extension for Applications Migrating to the Enterprise Data Center[3] (EDC). The IATO Extension memorandum was created to avoid expiration of the current BSM-E (FAS) IATO pending realignment of the system under the EDC SSAA. Furthermore, in September 2005, the DAA signed an ATO for the BSM-E (FAS) Base Level Support Application. According to NIST Special Publication 800-37, security reaccreditation occurs at the discretion of the authorizing official when significant changes have taken place in the information system or when a specified time period has elapsed in accordance with federal or agency policy. Between October 2003 and September 2005, BSM-E (FAS) underwent two major system changes; becoming a MAC II Sensitive System and separating the Base Level system from the rest of BSM-E (FAS), which required completion of a separate C&A for the Base Level system. However, the DAA did not require the completion of a full reaccreditation of the system in either of those instances.

[3] The EDC is a consolidation and outsourcing of DLA servers and database operations from the current multi-distributed data center approach to a logical Data Center using a geographically dispersed data center approach. These data centers are located in commercial facilities and are maintained by the contractor.

DLA should ensure that the BSM-E (FAS) system undergoes a full reaccreditation to include the BSM-E (FAS) Base Level Support Application in accordance with DoD 8510.1-M, which states as changes to a system occur, they should be reflected in the SSAA.

Plans of Action and Milestones. The BSM-E (FAS) POA&M did not address all BSM-E (FAS) security weaknesses and was not being updated on a quarterly basis. The OMB Memorandum 02-01, "Guidance for Preparing and Submitting Security POA&M," October 17, 2001, states that the purpose of a POA&M is to assist agencies in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for security weaknesses found in programs and systems. Additionally, the Memorandum states that agency officials should prepare a POA&M for every system for which weaknesses were identified in security act reports, audits, and assessments and should submit brief status updates of their system POA&Ms to their agency CIO on a quarterly basis.

As a result of a review by the Joint Interoperability Test Command in September 2003, DLA created the BSM-E (FAS) POA&M that included IA findings from the review. However, the BSM-E (FAS) POA&M did not address all IA findings. For example, the Joint Interoperability Test Command Report stated that the documentation provided in the SSAA did not contain the comprehensive elements of a system security plan that identifies the technical, administrative, and procedural IA program. The report specifically stated that DoD Instruction 8500.2 required the following elements to be documented:

- all external interfaces, the information being exchanged, and the protection mechanisms associated with the interface;
- user roles required for access control and the access privileges assigned to each role;
- unique security requirements;
- categories of sensitive information processed or stored by BSM-E (FAS) and their specific protection plans; and
- restoration priorities of subsystems, processes, or information.

As of June 2005, the BSM-E (FAS) POA&M did not include the task of updating the SSAA to reflect that documentation.

Additionally, the BSM-E (FAS) POA&M had not been updated since June 2005. According to DLA IA personnel, the POA&M will not be updated until the migration of BSM-E (FAS) to EDC, tentatively scheduled for January 2006. However, since the last POA&M update in June 2005, BSM-E (FAS) underwent a major architectural change when the Base Level system received its own separate accreditation in September 2005. Therefore, DLA should update the BSM-E (FAS) POA&M and remove weaknesses that pertained to the Base Level system.

User Access Controls. BSM-E (FAS) user access controls needed improvement at DLA and the Base Level user sites. Specifically, DLA did not require all BSM-E (FAS) users to implement necessary access controls and was unaware of who accessed BSM-E (FAS) at BSM-E (FAS) user sites. For example, DLA did not have procedures for granting and removing access to Base Level and FES users, completing user agreement forms at the Base Level, locking inactive computers, disabling inactive accounts, and accessing system software.

Base Level Users. The BSM-E (FAS) Base Level sites did not have user access and removal procedures. The three military sites visited did not have policies that outlined a process for granting access to new local area network users and therefore, access to BSM-E (FAS). Although two of the three military sites had policies that required new local area network users to complete an initial computer test before being granted access to the local area network, there was no consistency in how the three military sites granted access to new local area network users. Also, none of the three military sites had policies that outlined the requirements and duties for personnel that granted new BSM-E (FAS) users account access.

In addition, two of the three military sites visited did not have policies in place to remove Base Level system users from the network when access was no longer required. The third military site issued general guidance but did not identify specific duties. Each military site had an informal method for removing users, but had not established specific policies that outlined the removal process. As of January 2006, DLA did not know who had access to BSM-E (FAS) at the Base Level.

FES Users at Military Sites. DLA did not have procedures for removing individuals who no longer required access to FES at the Base Level. For example, for the three military sites visited, DLA headquarters had a list of all FES users at those sites; however, not all of the listed individuals who had FES access required FES access. Of the fifteen FES users listed at one site, three FES users no longer required FES access and three other FES users could not be found on the Global Address List. For the twenty FES users listed at the other two sites, each site had one person who could not be found on the Global Address List. If a user was not listed in the Global Address List, it meant they no longer had a network account at that location, and therefore, should no longer require access to the FES. DESC was developing an interim policy, DESC-T Instruction-24, which will outline the procedures for DESC user access to and removal from FES. However, until DESC-T Instruction-24 is approved, DESC does not have a policy that outlines the process to grant or remove DESC users access to BSM-E (FAS).

User Agreement Forms. Two of the three military sites and DLA headquarters require new network users to sign a User Agreement/Rules of Behavior document. The User Agreement/Rules of Behavior document outlines the standards of conduct that the user is expected to follow. The other military site did not implement or use a User Agreement/Rules of Behavior document for network users acknowledgement and agreement. DoD Instruction 8500.2, "IA Implementation," February 6, 2003, requires a set of rules that describes the responsibilities and expected behavior of all personnel, including the consequences for non-compliance with the rules. A signed acknowledgement of

the rules is a condition of access. Accordingly, DLA needs to direct all BSM-E (FAS) sites that use BSM-E (FAS) to comply with DoD Instruction 8500.2 and require users to sign a formal standardized User Agreement/Rules of Behavior document before gaining access to the system.

User Lockout. BSM-E (FAS) computers did not have a screen-lock function that prevented users access to the system after periods of inactivity. Specifically, network settings on the BSM-E (FAS) computers at the three military sites did not automatically log users off or lock them out of their workstation after a period of inactivity. At one military site, a Base Level computer activated a password protected screen saver after sitting inactive for a period of time; however, the setting on the computer was manually set. At two other military sites, Base Level computers did not use a screensaver lockout. There were no policies in place at any of the three military sites requiring a network setting for a log off or lock out function. Network technicians at DLA Headquarters stated that they had implemented a network setting that refreshes periodically on all user workstations at Headquarters to activate a password protected screen-saver on the user's workstation after a period of inactivity. However, DLA was not able to show the audit team an example of this network setting. Personnel at DLA advised that the newest version of BSM-E (FAS) (Fuels Manager Defense 6.0) will have a feature which will automatically log users out of BSM-E (FAS) after a period of inactivity, even if the user had not logged off their workstation. DoD Instruction 8500.2 requires the association of a screen-lock function with each workstation. The screen-lock function, when activated by either a specific user action or after a specified period of workstation inactivity (e.g., 15 minutes), places an unclassified pattern on the screen that hides the previously visible screen. Once the screen-lock function is activated, access to the workstation requires a unique authenticator. DLA should ensure a screen-lock function is installed on every workstation that runs BSM-E (FAS), as required by DoD Instruction 8500.2, because the system does not require an individual log-in to gain access to the system. Without a screen-lock function, potentially unauthorized individuals could gain access to BSM-E (FAS) on an unprotected workstation connected to a network.

Additionally, at two military sites, permission settings for BSM-E (FAS) were not limited to individuals who required access to BSM-E (FAS). At these two military sites, permission settings were set to allow everybody on the base with a network username and password to access BSM-E (FAS). When advised, personnel from DESC and the site were able to change the permission settings at one of the two locations. However, the other location still had permission settings that allowed everyone with a network account to have access to BSM-E (FAS). DLA should require all BSM-E (FAS) Base Level sites to evaluate their network permission settings to ensure that only current BSM-E (FAS) users have access to the system. Unnecessary or unauthorized access could pose undue risks to DoD systems and information.

Inactive Accounts. Inactive accounts were not being properly removed from the network. None of the military sites visited had a policy in place regarding the removal of inactive accounts. Also, one military site did not scan their network for inactive accounts. Another military site scanned the network quarterly and deactivated inactive accounts with the permission of the inactive

user's manager. The third military site scanned the network for accounts that had been inactive for at least 45 days and either deleted or disabled the account with the approval of the inactive user's manager. Any inactive account was deleted after 90 days of inactivity; however, none of these functions were documented in formal policy. DLA should require BSM-E (FAS) Base Level sites to disable or remove inactive accounts so there is no way for users to gain unauthorized access.

DLA is in the process of implementing a new process for handling inactive accounts on the DLA network. DLA plans to conduct monthly network scans to detect accounts that have been inactive for 90 days, which will then be deactivated. After 6 months of inactivity, the user's account will be archived and no longer accessible. Prior to this change, DLA only performed networks scans every 6 months. Although DLA's new process increases the number of scans for inactive accounts, the procedures do not meet One Book requirements. The DLA One Book, "Information Assurance Operational Controls," August 19, 2004, states that user accounts which exceed 30 days of inactivity will be disabled. DLA should ensure that inactive accounts are being disabled in accordance with the One Book policy.

Access to System Software. Critical software for BSM-E (FAS) must be kept safeguarded. The BSM-E (FAS) software has been well protected at DLA headquarters. While two of the three military sites visited stored the BSM-E (FAS) software disk in a locked location, the third military site stored the system software disk next to the computer in an unlocked container. Additionally, none of the three military sites stored the critical software in a fireproof container or at a separate location, as outlined in DoD Instruction 8500.2. DLA should ensure the BSM-E (FAS) software is stored at a separate location and in an appropriate container.

Annual Security Awareness Training. The BSM-E (FAS) users were not consistently provided annual security awareness training or required privileged user training. As required by DoD Directive 8570.1, "Information Assurance, Training, Certification, and Workforce Management," August 15, 2004, all users of DoD information systems shall receive initial IA awareness and annual IA refresher awareness training. Additionally, all privileged users shall be fully qualified, trained, and certified to DoD baseline requirements to perform their IA duties. The FISMA also requires all DoD Components to report training information annually to the OMB and Congress.

Required annual IA security awareness training was not being enforced. Based on a judgmental sample of users at each location visited, only one of the four sites, including DLA Headquarters, had updated their annual IA security awareness training for FY 2005. All three Base Level users at one military site completed their IA security awareness training. At the second military site, 23 of 36 Base Level users completed their required annual IA security awareness training. At the third military site, none of the three Base Level users completed their required annual IA security awareness training. Based on a judgmental sample of 20 of the 170 FES users at DLA headquarters, only 1 of the 20 people sampled completed their FY 2005 IA security awareness training as of October 13, 2005.

DLA did not track users with significant security responsibilities at the Base Level or whether those users had been properly trained. At each of the three military sites visited, there was one individual with significant security responsibilities who could make network and BSM-E (FAS) system changes. One of the three military sites had a checklist of training requirements for the position. Another of the three military sites had a one course minimum completion requirement for the individual to achieve their position. The third military site had no training requirements outlined for the individual with significant security responsibilities. DLA currently does not have a training plan in place that requires training for individuals with significant security responsibilities. However, DLA personnel reported that there is a Statement of Work in place with a contractor to develop an IT and IA Professional Development Plan which will outline required training, tasks, and skills for each job function at DLA.

Continuity of Operations Plans. DLA had not updated or tested the BSM-E (FAS) COOP since October 2004. According to DLA personnel, there are no plans to update or test the BSM-E (FAS) COOP until the system migrates to the EDC. DLA considers the migration of BSM-E (FAS) to EDC the next COOP test. However, since the last BSM-E (FAS) COOP test date occurred in October 2004 and the movement of BSM-E (FAS) to the EDC had a variable date of January 2006, DLA did not comply with the annual COOP test policy, as specified in the DLA One Book chapter, "IT COOP Planning," dated January 28, 2003. In addition, DLA did not know whether there was proper creation and storing of backup data or whether recovery procedures existed at the Base Level.

Update to COOP. DLA had not recently updated the BSM-E (FAS) COOP. The most recent version of the system COOP was dated October 2004, while the overall SSAA was last updated on April 27, 2005. As a result, there were discrepancies between the BSM-E (FAS) COOP and the SSAA. The Management Information software, one of the five primary software programs that make up the system, was not included in the COOP documentation. Additionally, the COOP contained an inaccurate Alternate Site point of contact list. DLA should review and update the BSM-E (FAS) COOP to correct its inconsistencies with the BSM-E (FAS) SSAA.

Testing of COOP. DLA had not recently tested the BSM-E (FAS) COOP. DLA had performed extensive two day COOP tests each year; however, the last test occurred in October 2004. DLA had developed an efficient and effective mirrored COOP site[4] for BSM-E (FAS). However, because DLA delayed the migration date of BSM-E (FAS) to the EDC numerous times, DLA did not know when the next COOP test of BMS-E (FAS) would take place; therefore, DLA was not compliant with their own COOP testing policy, which requires all IT COOP Plan processes to be tested annually. In addition, since the Base Level portion of BSM-E (FAS) did not have its own COOP, a Memorandum

[4] NIST Special Publication 800-34 states that mirrored sites are fully redundant facilities with full, real-time information mirroring, and are identical to the primary site in all technical respects. These sites provide the highest degree of availability because the data is processed and stored at the primary and alternate site simultaneously.

of Understanding/Agreement (MOU/A) should be in place between DLA and the Services stating that COOP testing of the system was the responsibility of DLA.

Backup and Recovery Procedures. DLA did not know if there was proper creation and storage of backup data for the Base Level system. At one of the three sites visited, the daily, weekly, and monthly backups of the fuels data were located in a small diskette box next to the main Base Level system computer terminal. According to the DESC Interim Procedures for Retention and Backup of Base Level Fuels Data, dated September 12, 2005, copies of the current daily and weekly Base Level system fuels data backup CDs/tapes should be stored in a suitable container at a location geographically separated from the Base Level system computer terminal. As of April 2006, there is no requirement for the Military Sites operating the Base Level system to adhere to DLA guidance, and therefore, the DESC Procedures are only used as a best practice at the Base Level. The DLA One Book Chapter, "IA Operational Controls, dated August 19, 2004, states that audit records for MAC II IT systems should be backed up daily. The One Book Chapter, "IT COOP Planning," also maintains that DLA should regularly perform data backups to avoid data loss and store current and archived backup data offsite.

Additionally, DLA did not efficiently provide updates of the DESC Interim Procedures for Retention and Backup of Base Level Fuels Data to the Base Level fuels personnel. One of the three sites visited used a version of the DESC Procedures that was over one year old. Updated versions of these procedures were placed on the DESC website; however, the Base Level users were not notified when those updates occurred. NIST Special Publication 800-18 states that backup procedures should be followed to ensure an application continues to be processed if the IT system becomes unavailable; backups should discuss frequency and scope of backing up data. DLA should notify the Base Level users when updates to the DESC Procedures occur to ensure the proper backup guidelines are being followed.

BSM-E (FAS) recovery procedures did not exist at the Base Level. None of the three sites visited had a formal contingency/recovery plan for BSM-E (FAS). Two of the sites did not have an established alternate processing facility for the Base Level system. DLA representatives explained that sites using BSM-E (FAS) are not required to develop a separate contingency/recovery plan for the Base Level system, even though one site did take responsibility to further secure the application. DLA and Base Level fuels personnel stated that the Base Level users will call the DESC Help Desk[5] with any questions or concerns about the Base Level system, even though there is no formal documentation telling them to do so. For example, the Base Level fuels personnel at one of the three sites visited encountered computer problems, which consisted of the two Base Level system computers randomly restarting. According to the Base Level fuels personnel, this was a reoccurring problem; however, no previous effort had been made to contact the DESC Help Desk to correct the problem. DLA should develop a MOU/A between DLA and the Services to ensure that Base Level system procedures for the Base Level system users are followed. Without an MOU/A between DLA and

[5] The DESC Help Desk is the primary source for reporting problems and obtaining assistance for problems related to DESC applications.

the Services, it is unclear who is responsible for recovery procedures at the Base Level.

Oversight of Information Assurance

The DLA One Book serves as the single authorized repository for Agency policies, processes, and procedures, and provides a mechanism for knowledge sharing within the Agency. Additionally, DLA determined that the One Book should be a major initiative in the internal process arena. By documenting its processes in the One Book, DLA wanted to achieve process management, improvement, and excellence. According to DLA, process documentation should be the foundation for having repeatable processes, for managing processes, and for having a baseline to improve upon.

IA Roles and Responsibilities. The DLA had not adequately defined processes and procedures in the One Book for ensuring that IA responsibilities were fulfilled. According to the DLA One Book Chapter, "Information Assurance (IA) Management Controls," dated August 2, 2004, the Chief of IA will develop DLA IA policies and guidelines and ensure Agency compliance. However, there has been no additional guidance issued by the Chief of IA with regards to information assurance responsibilities. In addition, the One Book policy needs updating to reflect the current organizational structure that the Chief of IA oversees.

Management Control Program. The DLA One Book assigns responsibilities to the DAA, the Chief of IA, the Program Manager or System Manager, the IA Manager, and the IA Officer. However, DLA has not instituted an effective Management Control Program to ensure personnel in each of those positions are completing their assigned responsibilities. Specifically regarding BSM-E (FAS), IA roles and responsibilities for the C&A of BSM-E (FAS) have not been clearly defined within the SSAA. Each BSM-E (FAS) Base Level operating location handles the BSM-E (FAS) user access controls differently. The current management of workstation settings, the removal of users and inactive accounts, access to software, and the training and documentation of qualified users puts BSM-E (FAS) information at risk of being accessed by non-authorized personnel. Additionally, there are no clearly defined roles at the Base Level for the continuity of system operations should the system fail. The DoD Instruction 8500.2 requires that information ownership responsibilities are established and that persons in those positions are held accountable for their assigned responsibilities. The DLA should create a control objective that ensures all parties responsible for the certification and accreditation of a system are completing the appropriate tasks efficiently and effectively.

The DLA's current assessment of its management controls includes an evaluation of the integrity of its automated information systems. According to DLA, users must have a logon identity and password for access to an information system. Currently, when accessing BSM-E (FAS) at the Base Level, a logon identity and password is not needed once a user is logged on to the site's local area network. With the full implementation of Fuels Manager Defense 6.0, all BSM-E (FAS)

users will be required to log into the Base Level portion of the system using an additional assigned logon identity and password.

DLA headquarters does not track who has access to BSM-E (FAS) at non-DLA locations. The J6F grants access to all FES users at DLA headquarters; however, once the FES users have access, DLA no longer consistently monitors the users. In addition, DESC does not monitor who has access to BSM-E (FAS) at the Base Level. Therefore, it is inaccurate for the J6F to report that the combination of a DESC login ID and secure passwords will prevent all unauthorized users from accessing the system. DLA does not know if users are denied system access when they no longer require access to BSM-E (FAS). As a result, the DLA valuation of the integrity of its Automated Information Systems is inadequate.

The J6F Management Control Program assessment reports that DLA performs biannual training of assigned functional area security personnel. However, DLA currently does not have a personnel training policy in place and is developing an IT and IA Professional Development Plan, which will outline training, skills, and tasks for all job functions at DLA.

Memorandum of Understanding/Agreements. The OMB Circular A-130, Appendix III requires that a system that interconnects with another system and shares information must have a system security plan that establishes controls consistent with the rules of the system and that are in accordance with guidance from NIST. Additionally, Appendix III requires agencies to obtain written management authorization before connecting their IT systems to other systems, based on an acceptable level of risk. NIST Special Publication 800-47, "Security Guide for Interconnecting IT Systems," dated August 2002, states that a system interconnection is defined as the direct connection of two or more IT systems for the purpose of sharing data and other information resources. According to NIST Special Publication 800-47, an organization that owns and operates a connected IT system should develop an Interconnection Security Agreement to document the technical requirements of the interconnection. A MOU/A should also be created that defines the responsibilities of the participating organizations.

DLA does not have an Interconnection Security Agreement or an MOU/A with the Services that allows the BSM-E (FAS) Base Level system to reside and operate on their local area networks; however, BSM-E (FAS) personnel have entrusted Service personnel to ensure operational controls are in place for BSM-E (FAS) at the Base Level. The DLA One Book does not address the completion of an Interconnection Security Agreement or an MOU/A in any of its policies on IA. In addition, the management control assessment of the integrity of information systems does not include a determination as to whether appropriate MOU/As are in place with Military Components that are operating DESC systems on their local area networks, as is the case with BSM-E (FAS).

Conclusion

BSM-E (FAS) is operating with vulnerabilities that present potential risks to the DLA and the DoD. Because BSM-E (FAS) is operating at non-DLA sites, the Agency should have an MOU/A with all the sites operating their system. The MOU/A should clearly delineate security safeguard responsibilities including the C&A of the Base Level sites and the local area networks that BSM-E (FAS) is operating on. Without a clearly defined agreement between the two organizations that own and operate the interconnected BSM-E (FAS) and the local area network, it is unclear what party should be establishing, operating, and securing the interconnection.

Additionally, the information being reported between DLA and the military services cannot be considered completely reliable while there is a risk of unauthorized access. Until DLA develops MOU/As that specifically outline the IA roles and responsibilities of DLA and the military services, BSM-E (FAS) information will be at risk and will not be secured to the fullest extent possible.

If BSM-E (FAS) users are not consistently provided annual security awareness training or required privileged user training, those individuals could either knowingly or inadvertently introduce security vulnerabilities into DoD networks. If personnel are not adequately informed of applicable organizational policy and procedures, they cannot be expected to effectively secure computer resources. In addition, if DLA does not have an accurate method to track who has received annual security awareness training, the agency is unable to know which employees could pose a serious threat to the security of their computer resources.

Without annual COOP testing, DLA cannot provide adequate assurance that the BSM-E (FAS), a MAC II system, will be able to recover from a system failure. The consequences of a system failure could delay or result in degradation of important support services or commodities that may seriously impact DoD mission effectiveness or operational readiness. Furthermore, without an MOU/A, there are no clearly defined responsibilities at the BSM-E (FAS) Base Level regarding the backup and recovery of the system, should a failure occur.

Recommendations, Management Comments, and Audit Response

1. We recommend that the Director, Defense Logistics Agency:

a. Require the Defense Logistics Agency Chief Information Officer/Designated Approving Authority to:

(1) Ensure the Business Systems Modernization-Energy (Fuels Automated System) completes a full certification and accreditation to include the Base Level Support Application;

Management Comments. The DLA CIO nonconcurred and stated that the DLA CIO/DAA has already accredited the BSM-E (FAS). The original BSM-E (FAS) ATO was issued on December 30, 2004, with an expiration date of June 28, 2007. The BSM-E (FAS) Base Level Support Application received a separate ATO on September 21, 2005, to support a Type Accreditation that expires on September 12, 2008.

Audit Response. The DLA CIO comments were nonresponsive. On December 30, 2004, the BSM-E (FAS) received an IATO, which expired on June 28, 2005. The initially requested ATO could not be granted based on outstanding IA items within the POA&M. Therefore, the BSM-E (FAS) has not been fully certified and accredited since 2001. In addition, on May 13, 2005, the DLA CIO/DAA issued an "Interim Approval to Operate Extensions for Applications Migrating to the Enterprise Data Center" pending the realignment of BSM-E (FAS) under the EDC. However, DLA has not determined when the migration to the EDC will occur. We request that DLA provide additional comments on the report.

(2) Develop information assurance policies and guidelines as required by the Defense Logistics Agency One Book; and

Management Comments. The DLA CIO nonconcurred and stated that the DLA CIO/DAA has published five One Book chapters to facilitate DLA's implementation of DoD IA requirements. The requirements included within these One Book chapters fully address the policies required to implement and sustain an effective IA Program.

Audit Response. The DLA CIO comments were nonresponsive. The DLA One Book chapter, "Information Assurance Management Controls," established the IA policy, requirements, and processes to implement, manage, and sustain an effective DLA IA program. The measurable output of this process is the implementation of a DLA IA program to ensure the confidentiality, integrity, availability, and non-repudiation of Sensitive But Unclassified and classified data processed and stored by IT systems. However, DLA has not effectively ensured the confidentiality, integrity, and availability of the information contained in systems that have received a type accreditation such as the BSM-E (FAS). (See Audit Response to Recommendation 1.a.3. below.) In addition, two of the five DLA One Book chapters referred to by DLA discuss the Chief of IA as part of the J-633 organization, which no longer exists in DLA. We request that DLA provide additional comments on the implementation and management of their IA program.

(3) Create a management control program that ensures compliance with all DoD and agency information assurance policies and guidelines.

Management Comments. The DLA CIO nonconcurred and stated that DLA has an effective IA management control program in place to ensure compliance with IA policies and guidelines. The IA Management Control One Book Chapter establishes responsibility for ensuring IA requirements are enforced by appropriate levels throughout the DLA organization. Also, IA Performance

Reviews are performed on a continuous basis to provide an independent assessment of the IA program implementation across the Agency. In addition, DLA commented that the Agency is not responsible for ensuring that Military Service personnel comply with DoD IA requirements. The BSM-E (FAS) Base Level Support Application Type Accreditation delineates Military Service personnel IA responsibilities and DLA does not have enforcement authority or responsibility for ensuring their compliance.

Audit Response. The DLA CIO comments were nonresponsive. DLA did not provide evidence that they conducted and completed IA Performance Reviews that provided an independent assessment of the IA program implementation across the Agency. Additionally, according to DoD 8510.1-M, an SSAA should be prepared for the system software and hardware considered under a type accreditation. The SSAA should be shipped to each prospective installation site with the software and hardware, where the site manager will receive confirmation and documentation of the C&A results and the equipment included in the SSAA. After installation of the information system, the type SSAA should be included in the network or site SSAA. However, DLA was unaware that the BSM-E (FAS) SSAA was not included in Base Level network SSAAs. Further, DoD 8510.1-M states that the information system facility and equipment must be under the control of the DAA. Any facility or equipment that is not considered or is not under the control of the DAA should be considered as an external interface. A description of the system's external interfaces should include the purpose of each external interface and the relationship between the interface and the system. The BSM-E (FAS) SSAA did not identify any external interfaces. We request that DLA provide the IA Performance Reviews that provide an independent assessment of the IA Program implementation across the Agency. We also request that DLA provide additional comments on the report.

b. Develop a Defense Logistics Agency plan of action and milestones pertaining to the significant management control weaknesses identified in 1.a. above and continue to report progress on corrective action to the Assistant Secretary of Defense for Networks and Information Integration on a quarterly basis, beginning March 2006, until all corrective actions are completed and verified, as required by the Federal Information Security Management Act.

Management Comments. The DLA CIO nonconcurred and stated that additional IA management controls are not required; therefore, there is no need to establish a POA&M or report on the implementation of controls that are currently in place.

Audit Response. The DLA CIO comments were nonresponsive. See Audit Response to Recommendation 1.a. above. According to the OMB Memorandum 05-15, "FY 2005 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management," June 13, 2005, program officials should develop a POA&M for all systems when an IT security weakness has been identified. The guidance directs CIOs and agency program officials to develop, implement, and manage an agency-wide POA&M process and incorporate all known IT security weaknesses associated with information systems used or operated by the agency. A status update of the system

performance metric must be submitted quarterly to OMB. The agency CIO centrally tracks, maintains, and reviews POA&M activities on at least a quarterly basis. In addition, OMB Memorandum 05-15 states that all agencies must implement the requirements of FISMA and report annually to OMB and Congress on the effectiveness of their security programs. We request that DLA provide additional comments on the report.

2. We recommend the Defense Logistics Agency Chief Information Officer/Designated Approving Authority:

a. Require the Information Operations Directorate, Fort Belvoir site, no later than May 2006, to:

(1) Update the Business Systems Modernization-Energy (Fuels Automated System) plan of action and milestones to include all security weaknesses based on the current system configuration;

Management Comments. The DLA CIO concurred and stated that corrective actions for the BSM-E (FAS) Base Level Support Application security vulnerabilities have been completed as part of Version 2.0 and are currently undergoing testing. An ATO to support Type Accreditation of Version 2.0 will be granted upon successful completion of this testing.

Audit Response. Although DLA concurred, we consider the DLA CIO comments nonresponsive because DLA referenced an outdated POA&M and did not discuss the most current version of the POA&M, dated June 2005, which was provided to the audit team during the audit. We request that DLA provide an updated POA&M that specifically details the corrective actions that have occurred on the ten deficiencies identified in the June 2005 POA&M. In addition, the updated POA&M should include all other outstanding deficiencies, corrective actions planned, and the expected date of the corrective actions.

(2) Create formal procedures for granting of access and removal of Business Systems Modernization-Energy (Fuels Automated System) Base Level users and Fuels Enterprise Server users at the Base Level;

Management Comments. The DLA CIO concurred and stated that the DLA CIO/DAA will direct J6F to take actions to implement appropriate measures for granting user access to the FES. However, J6F is not responsible for ensuring implementation of appropriate measures for granting user access to the BSM-E (FAS) Base Level Support Application. Under provisions within the Type Accreditation, this responsibility rests with the respective operational organizations as stipulated in BSM-E (FAS) Base Level Support Application SSAA.

Audit Response. Although the DLA CIO concurred with regard to FES users, we consider the comments regarding Base Level BSM-E (FAS) users nonresponsive. According to DoD 8510.1-M, the type accreditation SSAA must clearly define the system operating environment. The BSM-E (FAS) Base Level Support Application ATO, signed by the DAA, should have included a statement

that the system was granted a type accreditation and that the operators assume the responsibility to monitor the operational environment for compliance with that environment as described in the accreditation documentation. However, it did not. Additionally, DoD 8510.1-M requires the program manager, user representative, and information system security officer to ensure proper security operating procedures, configuration guidance, and training is delivered with the system. However, DLA did not develop or provide specific guidance to the Base Level system personnel regarding the granting of access and removal of BSM-E (FAS) Base Level users and FES users at the Base Level. We request DLA provide additional comments on the report.

(3) Create a formal and standard User Agreement/Rules of Behavior document before allowing access to Business Systems Modernization-Energy (Fuels Automated System);

Management Comments. The DLA CIO nonconcurred and stated that the IA Rules of Behavior Process One Book Chapter includes appropriate agreements for different levels of DLA system users, who are required to sign the agreement acknowledging receipt and understanding prior to being granted system access. The DLA CIO/DAA will continue to emphasize compliance with the One Book Chapter for all Fuels Enterprise Server users. However, DLA is not responsible for ensuring that Military Service personnel comply with DLA policy for granting access to the BSM-E (FAS) Base Level Support Application.

Audit Response. The DLA CIO comments were nonresponsive. There are FES users at the Base Level; therefore, those FES users must follow the DLA IA Rules of Behavior Process One Book Chapter. DLA is responsible for ensuring the FES users at the Base Level comply with the DLA policy for granting access to BSM-E (FAS). In order for DLA to ensure FES user compliance with the One Book policies, an MOU/A needs to be created and implemented between DLA and the Services. OMB Memorandum 05-15 states that for non-national security programs and systems, agencies must follow NIST standards and guidelines. According to NIST SP 800-47, federal agencies must establish interconnection agreements. Also, OMB Circular A-130, Appendix III, requires agencies to obtain written management authorization before connecting their IT systems to other systems, based on an acceptable level of risk. The written authorization should define the rules of behavior and controls that must be maintained for the system interconnection and it should be included in the organization's system security plan. Additionally, NIST SP 800-47 states that an MOU/A defines the purpose of the interconnection; identifies relevant authorities; specifies the responsibilities of both organizations; and defines the terms of agreement. Therefore, DLA must create an MOU/A with the Services operating BSM-E (FAS) in order to establish responsibility and define the rules of behavior for BSM-E (FAS) Base Level users. We request that DLA provide additional comments on the report.

(4) Update the Business Systems Modernization-Energy (Fuels Automated System) continuity of operations plan to correct inconsistencies with the Business Systems Modernization-Energy (Fuels Automated System) System Security Authorization Agreement; and

Management Comments. The DLA CIO concurred and stated that the BSM-E (FAS) application is currently in the process of transitioning to the DLA EDC. As a result of this transition, the current BSM-E (FAS) COOP is being updated for integration into the new DLA EDC computing environment. Finalization of this COOP update and associated testing are contingent upon completion of the BSM-E (FAS) application migration activities.

Audit Response. Although the DLA CIO concurred, we consider the comments partially responsive. DLA does not have a specific date as to when BSM-E (FAS) will migrate to the EDC; therefore, there is no definitive date for updating the BSM-E (FAS) COOP, which was last updated in October 2004. The date of the EDC transition has changed numerous times since October 2005 and DLA is unable to determine when the migration will occur. We recommend that the CIO/DAA require the Information Operations Directorate, Fort Belvoir (J6F) to establish a realistic date for the BSM-E (FAS) migration to the EDC and update the COOP to be in adherence with the BSM-E (FAS) SSAA. We request that DLA provide additional comments to this report.

(5) Perform a complete test of the continuity of operations plan for Business Systems Modernization-Energy (Fuels Automated System).

Management Comments. The DLA CIO concurred and stated that the BSM-E (FAS) application is currently in the process of transitioning to the DLA EDC. As a result of this transition, the current BSM-E (FAS) COOP is being updated for integration into the new DLA EDC computing environment. Finalization of this COOP update and associated testing are contingent upon completion of the BSM-E (FAS) application migration activities.

Audit Response. Although the DLA CIO concurred, we consider the comments only partially responsive. DLA does not have a specific date as to when BSM-E (FAS) will migrate to the EDC; therefore, there is no definitive date for testing the BSM-E (FAS) COOP. The date of the transition to the EDC has changed numerous times since October 2005 and DLA is unable to determine when the migration will occur. We recommend that the CIO/DAA require the Information Operations Directorate, Fort Belvoir (J6F) to establish a realistic date for the BSM-E (FAS) migration to the EDC and perform a complete test of the COOP.

3. We recommend the Information Operations Directorate, Fort Belvoir, no later than May 2006, create a Memorandum of Understanding/Agreement with the Business Systems Modernization-Energy (Fuels Automated System) Base Level user sites that defines the responsibilities for:

a. Ensuring a screen-lock function is installed on every workstation that runs Business Systems Modernization-Energy (Fuels Automated System).

Management Comments. The DLA CIO nonconcurred and stated that they have included the appropriate IA operational requirements within the BSM-E (FAS) Base Level Support Application SSAA in accordance with the provisions of DoD 8510.1-M, paragraph C3.3.5, for Type Accreditation. The SSAA supporting Type Accreditation eliminates the need for a separate MOU/A between DLA and

BSM-E (FAS) Base Level user sites. The provisions within the BSM-E (FAS) Base Level Support Application SSAA are binding on all organizations where the application is installed and operated. Military Service organization can opt to separately accredit the BSM-E (FAS) Base Level Support Application if they choose not to comply with the Type Accreditation requirements.

Audit Response. The DLA CIO comments were nonresponsive. According to OMB Memorandum 05-15, agencies must follow NIST standards and guidelines for non-national security programs and systems. Therefore, according to NIST SP 800-47, organizations that own and operate connected systems should establish an MOU/A (or equivalent document) that defines the responsibilities of both parties in establishing, operating, and securing the interconnection. More specifically, the MOU/A defines the purpose of the interconnection; identifies relevant authorities; specifies the responsibilities of both organizations; and defines the terms of agreement. DLA did not establish MOU/As with the Services that would allow the BSM-E (FAS) Base Level system to reside and operate on their local area networks. Additionally, the BSM-E (FAS) Base Level Support Application Environment Description contained in the SSAA does not comply with DoD 8510.1-M, paragraph C3.3.3.5. (the paragraph C.3.3.5. referenced in the DLA response does not exist and may be a typo), which states that a type accreditation SSAA should define the intended operating environment as well as any operating procedures required for the type accredited system. The BSM-E (FAS) Base Level Support Application SSAA does not specifically state that a screen lock function should be installed on every workstation that runs BSM-E (FAS). The DoD 8510.1-M states that the program manager, user representative, and information system security officer should ensure that the proper security operating procedures, configuration guidance, and training is delivered with the system. The Information Operations Directorate, Fort Belvoir (J6F), did not take steps to define proper security operating procedures; did not provide proper configuration for the BSM-E (FAS); and did not administer security training to the Base Level users. Further, DoD 8510.1-M requires the type accreditation SSAA be shipped to each prospective installation site with the intention of the system SSAA being included in the site SSAA; however, there was no evidence that the BSM-E (FAS) SSAA was included in the Base Level site SSAA at any of the visited military sites. We request that DLA provide additional comments to the report.

b. Evaluating network settings at Base Level sites to ensure that only current users have access to Business Systems Modernization-Energy (Fuels Automated System).

Management Comments. The DLA CIO nonconcurred and stated that they have included the appropriate IA operational requirements within the BSM-E (FAS) Base Level Support Application SSAA in accordance with the provisions of DoD 8510.1-M. The SSAA supporting Type Accreditation eliminates the need for a separate MOU/A between DLA and BSM-E (FAS) Base Level user sites. The provisions within the BSM-E (FAS) Base Level Support Application SSAA are binding on all organizations where the application is installed and operated. Military Service organizations can opt to separately accredit the BSM-E (FAS) Base Level Support Application if they choose not to comply with the Type Accreditation requirements.

Audit Response. The DLA CIO comments were nonresponsive. See Audit Response to Recommendation 3.a. above. Additionally, the BSM-E (FAS) Base Level Support Application SSAA does not define responsibilities for evaluating network settings at Base Level sites to ensure that only current users have access to BSM-E (FAS). We request that DLA provide additional comments to the report.

c. Creating a formal policy for the removal of inactive accounts after 30 days of inactivity.

Management Comments. The DLA CIO nonconcurred and stated that they have included the appropriate IA operational requirements (to include account control) within the BSM-E (FAS) Base Level Support Application SSAA in accordance with the provisions of DoD 8510.1-M. The SSAA supporting Type Accreditation eliminates the need for a separate MOU/A between DLA and BSM-E (FAS) Base Level user sites. The provisions within the BSM-E (FAS) Base Level Support Application SSAA are binding on all organizations where the application is installed and operated. Military Service organizations can opt to separately accredit the BSM-E (FAS) Base Level Support Application if they choose not to comply with the Type Accreditation requirements.

Audit Response. The DLA CIO comments were nonresponsive. See Audit Response to Recommendation 3.a. above. Additionally, the BSM-E (FAS) Base Level Support Application SSAA does not contain a policy for the removal of inactive accounts after 30 days of inactivity. We request that DLA provide additional comments to the report.

d. Requiring Base Level users to ensure that Business Systems Modernization-Energy (Fuels Automated System) software is stored at a location separate from the operating location and in an appropriate container.

Management Comments. The DLA CIO nonconcurred and stated that they have included the appropriate IA operational requirements (to include continuity of operations) within the BSM-E (FAS) Base Level Support Application SSAA in accordance with the provisions of DoD 8510.1-M. The SSAA supporting Type Accreditation eliminates the need for a separate MOU/A between DLA and BSM-E (FAS) Base Level user sites. The provisions within the BSM-E (FAS) Base Level Support Application SSAA are binding on all organizations where the application is installed and operated. Military Service organization can opt to separately accredit the BSM-E (FAS) Base Level Support Application if they choose not to comply with the Type Accreditation requirements.

Audit Response. The DLA CIO comments were nonresponsive. See Audit Response to Recommendation 3.a. above. Additionally, the BSM-E (FAS) Base Level Support Application SSAA does not require Base Level users to ensure the BSM-E (FAS) backup software is stored at a location separate from the operating location and in an appropriate container. We request that DLA provide additional comments to the report.

e. Ensuring Business Systems Modernization-Energy (Fuels Automated System) users are provided annual security awareness training consistent with the requirements in DoD Directive 8570.1.

Management Comments. The DLA CIO nonconcurred and stated that the Military Service personnel at BSM-E (FAS) Base Level user sites should have received security awareness training as a prerequisite to gaining local area network access, as required by DoDI 8500.2. DLA is responsible for and includes training on the application security controls as part of its normal BSM-E (FAS) Base Level Support Application user training.

Audit Response. The DLA CIO comments were nonresponsive. According to DoD 8510.1-M, for a type accreditation, the DAA should include a statement in the accreditation memorandum that declares the system is granted a type accreditation and the operator must assume the responsibility to monitor the environment for compliance with the environment as described in the accreditation documentation. DLA did not include a similar statement in the BSM-E (FAS) Base Level Support Application SSAA. Further, DLA should ensure that the proper security operating procedures, configuration guidance, and training is delivered with the system to the Base Level sites, as required by DoD 8510.1-M. DLA did not provide training guidance to the Base Level operating sites for granting Base Level BSM-E (FAS) users access to the system. We request that DLA provide additional comments on the report.

f. Tracking users with significant security responsibilities and ensure those users are being properly trained consistent with the requirements in DoD Directive 8570.1.

Management Comments. The DLA CIO nonconcurred and stated that the Military Service personnel at BSM-E (FAS) Base Level user sites should have received security awareness training as a prerequisite to gaining local area network access, as required by DoDI 8500.2. DLA is responsible for and includes training on the application security controls as part of its normal BSM-E (FAS) Base Level Support Application user training.

Audit Response. The DLA CIO comments were nonresponsive. According to DoD 8510.1-M, for a type accreditation, the DAA should include a statement in the accreditation memorandum that declares the system is granted a type accreditation and the operator must assume the responsibility to monitor the environment for compliance with the environment as described in the accreditation documentation. DLA did not include a similar statement in the BSM-E (FAS) Base Level Support Application SSAA. Further, DLA should ensure that the proper security operating procedures, configuration guidance, and training is delivered with the system to the Base Level sites, as required by DoD 8510.1-M. DLA did not provide training guidance to the Base Level operating sites for granting Base Level BSM-E (FAS) users access to the system. We request that DLA provide additional comments on the report.

g. Ensuring backup and recovery procedures exist and are being followed at the Business Systems Modernization-Energy (Fuels Automated System) Base Level.

Management Comments. The DLA CIO nonconcurred and stated that they have included the appropriate IA operational requirements (to include continuity of operations) within the BSM-E (FAS) Base Level Support Application SSAA in accordance with the provisions of DoD 8510.1-M. The SSAA supporting Type Accreditation eliminates the need for a separate MOU/A between DLA and BSM-E (FAS) Base Level user sites. The provisions within the BSM-E (FAS) Base Level Support Application SSAA are binding on all organizations where the application is installed and operated. Military Service organization can opt to separately accredit the BSM-E (FAS) Base Level Support Application if they choose not to comply with the Type Accreditation requirements.

Audit Response. The DLA CIO comments were nonresponsive. See Audit Response to Recommendation 3.a. above. Additionally, the BSM-E (FAS) Base Level Support Application SSAA does not require BSM-E (FAS) Base Level users to ensure backup and recovery procedures exist and are being followed at the BSM-E (FAS) Base Level operating sites. We request that DLA provide additional comments to the report.

Appendix A. Scope and Methodology

We searched the DoD Information Technology Registry in March 2005 for DLA information systems designated as Mission Critical and MAC I or II. We selected the BSM-E (FAS), a Mission Critical, MAC II system, for review.

We assessed the information security operational controls for the BSM-E (FAS). We visited and interviewed personnel at the DLA Headquarters, Fort Belvoir, Virginia; Charleston Air Force Base, Charleston, South Carolina; Beaufort Marine Corps Air Station, Beaufort, South Carolina; Fort Hood Army Base, Killeen, Texas; the Defense Supply Center Richmond, Richmond, Virginia; and the Washington Navy Yard, Washington, D.C. Throughout the site visits and interviews, we evaluated the certification and accreditation for BSM-E (FAS), the system security plan, risk assessment, user access, security awareness and training, and continuity of operations and disaster recovery of BSM-E (FAS).

We reviewed Federal laws, OMB guidance, NIST guidance, and DoD Directives, Instructions, and Memoranda. We also reviewed the BSM-E (FAS) SSAA dated April 27, 2005; the BSM-E (FAS) COOP dated October 2004; the DESC Interim Procedures for Retention and Backup of Base Level Fuels Data, dated September 12, 2005; the DESC Interim Procedures for Requesting Access to DESC Automated Information System Applications, dated July 1, 2005; and the DLA One Book Chapters discussing IT COOP Planning; IA Rules of Behavior Process; IA Operational Controls; and IA Management Controls.

We performed this audit from April 2005 through January 2006 in accordance with generally accepted government auditing standards.

Use of Computer-Processed Data. We did not use computer-processed data to perform this audit.

Government Accountability Office High-Risk Area. The Government Accountability Office has identified several high-risk areas in DoD. This report provides coverage of the Protecting the Federal Government's Information-Sharing Mechanisms and the Nation's Critical Infrastructures high-risk area.

Appendix B. Prior Coverage

During the last five years, the DoD IG and Government Accountability Office have issued eight reports related to information security operational controls within the DoD and DLA. Unrestricted Government Accountability Office reports can be accessed over the Internet at http://www.gao.gov. Unrestricted DoD IG reports can be accessed at http://www.dodig.mil/audit/reports.

GAO

GAO Report No. GAO-06-31, "Information Security: The Defense Logistics Agency Needs to Fully Implement Its Security Program," October 7, 2005

DoD IG

DoD IG Report No. D-2006-042, "Security Status for Systems Reported in DoD Information Technology Databases," December 20, 2005

DoD IG Report No. D-2005-110, "Summary of Information Security Weaknesses Reported by Major Oversight Organizations from August 1, 2004, through July 31, 2005," September 23, 2005

DoD IG Report No. D-2005-099, "Status of Selected DoD Policies on Information Technology Governance," August 19, 2005

DoD IG Report No. D-2005-094, "Proposed DoD Information Assurance Certification and Accreditation Process," July 21, 2005

DoD IG Report No. D-2005-054, "Audit of the DoD Information Technology Security Certification and Accreditation Process," April 28, 2005

DoD IG Report No. D-2005-029, "Management of Information Technology Resources Within DoD," January 27, 2005

DoD IG Report No. D-2005-025, "DoD FY 2004 Implementation of the Federal Information Security Management Act for Information Technology Training and Awareness," December 17, 2004

Appendix C. Criteria

Federal Guidance

Public Law 100-235, "Computer Security Act of 1987." This law requires each Federal Agency to identify each computer system that contains sensitive information. In addition, the law requires agencies to develop a security plan for each computer system. Each Federal agency shall provide for the mandatory periodic training in computer security awareness and accepted computer security practice of all employees who are involved with each Federal computer system of that agency.

OMB Circular No. A-130, Appendix III, "Security of Federal Automated Information Resources," November 2000. Appendix III of OMB Circular A-130 states that agencies shall implement and maintain an automated information security program to assure that adequate security is provided for all agency information collected, processed, transmitted, stored, or disseminated in general support systems and major applications. The information security program helps to ensure controls were adequate, properly implemented, and applied consistently across the entity and information security responsibilities were clearly understood.

NIST Guidance. FISMA amends section 20 of the NIST Act (15 United States Code 278g-3) and, among other things, requires NIST to have the mission of providing adequate information security for all agency operations and assets; however, such standards and guidelines shall not apply to national security systems. The standards and guidelines include, at a minimum, standards for categorizing agency information and information systems and minimum information security requirements for information and information systems in each area.

NIST 800-26. NIST Special Publication 800-26, "Security Self-Assessment Guide for IT Systems," November 2001, builds on the Federal IT Security Assessment Framework developed by NIST for the Federal Chief Information Officer (CIO) Council. The Framework establishes a standardized measurement of security status and criteria that agencies could use to determine if security measures were adequately implemented. Additionally, NIST Special Publication 800-26 provides guidance on applying the Framework by identifying several control areas, such as those pertaining to system security plans, access controls, and contingency planning.

NIST 800-34. NIST Special Publication 800-34, "Contingency Planning Guide for Information Technology Systems," June 2002, provides instructions, recommendations, and considerations for government IT contingency planning. According to this guide, contingency planning involves establishing thorough plans and procedures to enable a system to be recovered quickly and effectively following a service disruption or disaster. Contingency planning generally includes restoring IT operations at an alternate location; or recovering IT

operations using alternate equipment; or performing some or all of the affected business processes using non-IT (manual) means. A COOP involves restoring an organization's essential elements at an alternate site and performing those functions for up to 30 days before returning to normal operations. The IT Contingency Planning Process contains seven steps: develop the contingency planning policy statement; conduct the business impact analysis; identify preventative controls; develop recovery strategies; develop an IT contingency plan; plan testing, training, and exercises; and plan maintenance.

NIST 800-47. NIST Special Publication 800-47, "Security Guide for Interconnecting Information Technology Systems," August 2002, provides a "life-cycle management" approach for interconnecting IT systems, with an emphasis on security. The approach includes four phases: planning, establishing, maintaining, and disconnecting the interconnection. The document describes various benefits of interconnecting IT systems, identifies the basic components of an interconnection, identifies methods and levels of interconnectivity, and discusses potential security risks associated with an interconnection. The document also contains guides and samples for developing an Interconnection Security Agreement, MOU/A and a System Implementation Plan. The MOU/A defines the purpose of the interconnection, identifies relevant authorities, specifies responsibilities of both organizations, and defines the terms of agreement.

NIST 800-53. NIST Special Publication 800-53, "Recommended Security Controls for Federal Information Systems," February 2005, provides guidelines for selecting and specifying security controls for information systems supporting the executive agencies of the federal government and is intended to provide guidance until the publication of Federal Information Processing Standards 200, "Minimum Security Controls for Federal Information Systems," in December 2005. The minimum assurance requirements for these security controls are grouped by a security control baseline; low, moderate, and high. In addition, this document contains a security control catalog which outlines the controls, supplemental guidance, and control enhancements for families of security controls. The families of security controls which are covered include: access controls; awareness and training; certification, accreditation, and security assessments; configuration management; contingency planning; identification and authentication; incident response; physical and environmental protection; planning; personnel security; risk assessment; system and communications protection.

DoD Guidance

DoD Instruction 5200.40, "DoD IT and Security Certification and Accreditation Process, December 30, 1997. This instruction implements policy, assigns responsibilities, and prescribes procedures under DoD Directive 5200.28, "Security Requirements for Automated Information Systems," March 21, 1988, for C&A of IT, including automated information systems, networks, and sites in the DoD. It also creates DoD 8510.1, "DoD IT and Security Certification and Accreditation Process Application Manual," July 2000, for security C&A of

unclassified and classified IT as well as stresses the importance of a life-cycle management approach to the C&A and reaccreditation of DoD IT.

DoD 8510.1-Manual, "DoD IT and Security Certification and Accreditation Process Application Manual," July 31, 2000. This manual is issued under the authority of DoD Instruction 5200.40, "DoD IT and Security Certification and Accreditation Process," December 30, 1997. The DoD IT and Security Certification and Accreditation Process establishes a standard process, set of activities, general tasks, and a management structure to certify and accredit information systems that will maintain the information assurance and security posture of the Defense Information Infrastructure. This manual provides implementation guidance to standardize the certification and accreditation process throughout DoD and is mandatory for use by all DoD Components. It breaks the process into 4 phases. Phases 2, 3, and 4 are related to security and contingency plans.

DoD Directive 8500.1, "Information Assurance (IA)," October 24, 2002. This directive establishes policy and assigns responsibilities to achieve DoD IA. This directive requires all DoD information systems to maintain an appropriate level of confidentiality, integrity, authentication, non-repudiation and availability. DoD Directive 8500.1 requires adequate training of all personnel authorized access to DoD information systems and states that the minimum requirement for DoD information access should be a properly administered and protected individual identifier and password.

DoD Instruction 8500.2, "Information Assurance (IA) Implementation," February 6, 2003. This Instruction implements policies and procedures and assigns responsibilities for applying integrated, layered protection for DoD information systems and networks. DoD Instruction 8500.2 requires that all DoD information systems operate effectively and provide appropriate confidentiality, integrity, and availability. The Component Head should also ensure that IA awareness, training, education, and professionalization are provided to all military and civilian personnel, including contractors, commensurate with their respective responsibilities for developing, using, operating, administering, maintaining, and retiring DoD information systems. The Assistant Secretary of Defense for Command, Control, Communications, and Intelligence, as the DoD CIO, shall establish a DoD core curriculum for IA training and awareness and provide oversight of DoD IA education, training, and awareness activities.

DoD Instruction 8500.2 requires the use of an individual identifier and password to gain access to a DoD information system. Registration to receive a user ID and password includes authorization by a supervisor and is done in person before a designated registration authority. Also required as part of MAC II system controls for integrity and availability, is a set of rules that describe the IA operations of the DoD information system and clearly delineate IA responsibilities and expected behavior of all personnel, including the consequences of inconsistent behavior or non-compliance. A workstation screen-lock functionality should also be implemented at each workstation as part of these controls.

DoD Directive 8570.1, "Information Assurance (IA) Training, Certification, and Workforce Management," August 15, 2004. This directive establishes policy and assigns responsibilities in accordance with IA in the DoD. DoD Directive 8570.1 requires that all employees with IA responsibilities be identified, tracked, and managed so that trained individuals are working at each function level. All authorized users of DoD Information Systems shall receive initial IA awareness orientation as a condition of access and thereafter must complete annual IA refresher awareness. Privileged users and IA managers shall be fully qualified, trained, and certified to DoD baseline requirements to perform their IA duties.

DoD Directive 3020.26, "Defense Continuity Program," September 8, 2004. This directive establishes the Defense Continuity Program, revises continuity policies, and assigns responsibilities to high-ranking officials for developing and maintaining the Defense Continuity Program. According to this Directive, the DoD shall have a comprehensive and effective Defense Continuity Program that ensures DoD Component mission essential functions continue under all circumstances. Also, the performance of mission essential functions in a continuity threat or event shall be the basis for continuity planning, preparation, and execution. This directive orders the Head of the DoD Components to develop, coordinate, and maintain continuity plans and to update and reissue plans every two years. Also, the Head of the DoD Components should test and exercise continuity plans at least annually, or otherwise as directed; identify relocation sites or platforms for use during continuity threats or events; and provide for the identification, storage, protection, and availability for use at relocation sites, the vital records, materiel, and databases required to execute mission essential functions.

DLA Guidance

DLA Directive 5025.30, The DLA One Book. The DLA One Book Chapters were developed as a knowledge sharing single authorized repository for agency policies, processes, and procedures. The intent of the IA Operational Controls and IA Management Controls chapters of the DLA One Book is to establish the IA policy, requirements, and processes to implement, manage, and sustain an effective DLA IA Program. The DLA IT COOP Planning Chapter requires each DLA J6 Field Site to: perform IT COOP planning, minimize risk of losing processing capability, and ensure they have the ability to recover following loss of operational capability. In addition, it is DLA policy that all persons requiring access to DLA IT systems read, understand, and formally acknowledge the DLA IA Rules of Behavior prior to being granted initial IT system access or prior to a change in IT system access privileges.

DLA Interim Procedures. The DESC Interim Procedures for Retention and Backup of Base Level Fuels Data provides data backup procedures, general procedures for archiving and restoring data files, and conforming electronic data storage and retention procedures to Federal and DoD policy guidelines and National Archive Standards. Additionally, the Interim Procedures for Requesting Access to DESC Automated Information System Applications provide instruction

to personnel requiring access to any DESC Automated Information System Application by submitting a requirement for system access.

Appendix D. Report Distribution

Office of the Secretary of Defense

Under Secretary of Defense for Acquisition, Technology, and Logistics
    Deputy Under Secretary of Defense (Business Transformation)
Under Secretary of Defense (Comptroller)/Chief Financial Officer
    Deputy Under Secretary of Defense (Financial Management)
Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer
Chief Information Officer, Office of the Secretary of Defense

Joint Staff

Director, Joint Staff
Chief Information Officer, Joint Staff

Department of the Army

Chief Information Officer, Department of the Army
Auditor General, Department of the Army

Department of the Navy

Chief Information Officer, Department of the Navy
Naval Inspector General
Auditor General, Department of the Navy

Department of the Air Force

Chief Information Officer, Department of the Air Force
Auditor General, Department of the Air Force

Unified Commands

Chief Information Officer, U.S. Central Command
Chief Information Officer, U.S. European Command
Chief Information Officer, U.S. Joint Forces Command
Chief Information Officer, U.S. Northern Command
Chief Information Officer, U.S. Pacific Command
Chief Information Officer, U.S. Southern Command
Chief Information Officer, U.S. Special Operations Command
Chief Information Officer, U.S. Strategic Command
Chief Information Officer, U.S. Transportation Command

Other Defense Organizations

Director, Defense Logistics Agency
Chief Information Officer, American Forces Information Service
Chief Information Officer, Defense Advanced Research Projects Agency
Chief Information Officer, Defense Commissary Agency
Chief Information Officer, Defense Contract Audit Agency
Chief Information Officer, Defense Contract Management Agency
Chief Information Officer, Defense Finance and Accounting Agency
Chief Information Officer, Defense Human Resource Activity
Chief Information Officer, Defense Information Systems Agency
Chief Information Officer, Defense Logistics Agency
Chief Information Officer, Defense Security Cooperation Agency
Chief Information Officer, Defense Security Service
Chief Information Officer, Defense Technical Information Center
Chief Information Officer, Defense Technology Security Administration
Chief Information Officer, Defense Threat Reduction Agency
Chief Information Officer, Department of Defense Education Activity
Chief Information Officer, Department of Defense Inspector General
Chief Information Officer, DoD Test Resources Management Center
Chief Information Officer, Missile Defense Agency
Chief Information Officer, Pentagon Force Protection Agency
Chief Information Officer, TRICARE Management Agency
Chief Information Officer, U.S. Mission North Atlantic Treaty Organization
Chief Information Officer, Washington Headquarters Service

Non-Defense Federal Organization

Office of Management and Budget

Congressional Committees and Subcommittees, Chairman and Ranking Minority Member

Senate Committee on Appropriations
Senate Subcommittee on Defense, Committee on Appropriations
Senate Committee on Armed Services
Senate Committee on Homeland Security and Governmental Affairs
House Committee on Appropriations
House Subcommittee on Defense, Committee on Appropriations
House Committee on Armed Services
House Committee on Government Reform
House Subcommittee on Government Efficiency and Financial Management, Committee on Government Reform
House Subcommittee on National Security, Emerging Threats, and International Relations, Committee on Government Reform
House Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census, Committee on Government Reform

Defense Logistics Agency Comments

DEFENSE LOGISTICS AGENCY
HEADQUARTERS
8725 JOHN J. KINGMAN ROAD
FORT BELVOIR, VIRGINIA 22060-6221

IN REPLY REFER TO J-65

FEB 28 2006

MEMORANDUM FOR PROGRAM DIRECTOR, ACQUISITION AND TECHNOLOGY MANAGEMENT, DEPARTMENT OF DEFENSE INSPECTOR GENERAL
ATTN: MS. KATHRYN M. TRUEX

SUBJECT: Draft Report on "Review of the Information Security Operational Controls of the Defense Logistics Agency's Business Systems Modernization – Energy" (Project No. D2005-D000AL-0158.000)

DLA has reviewed the draft Department of Defense Inspector General report on Business Systems Modernization-Energy (BSM-E) and nonconcurs with the majority of recommendations and concurs with comments on the remainder. The basis for this position is that findings and recommendations within the report do not recognize or acknowledge provisions within DOD policy (i.e., DOD 8510.1-M). This policy assigns security operational control governance authority to organizations responsible for day-to-day operation of Type Accredited systems. We acknowledge that individuals at several BSM-E Base Level Support Application operational sites failed to implement or ensure compliance with applicable DOD Information Assurance requirements. However, it is DOD policy, per DOD 8510.1-M, that the operating activity insure appropriate information security operational controls are in place. Corrective action for many of the findings and recommendations within this report should be addressed to the appropriate Military Service organization for resolution.

A matrix of the recommendations and our responses is attached. The point of contact for this effort is Ms. Brandi Griffith, J-651, (703) 767-1910, or e-mail: brandi.griffith@dla.mil.

MAE DE VINCENTIS
Director, Information Operations
Chief Information Officer

Attachment

cc:
OASD(NII)

Federal Recycling Program Printed on Recycled Paper

Department of Defense Office of Inspector General (DODOIG) Audit
Review of the Information Security Operational Controls of the Defense Logistics Agency's
Business Systems Modernization-Energy
Comment Matrix on the Recommendations
February 21, 2006

		DLA Response
DODIG Recommendations	**DLA Response**	**Remarks/Rationale**
1a. That the Director, DLA, require the CIO/DAA to ensure that the BSM-E completes a full certification and accreditation to include Base Level Support Application.	Nonconcur	The reason for nonconcurrence with this recommendation is that the DLA CIO/DAA has already accredited BSM-E. The original BSM-E (FAS) Authority to Operate (ATO) was issued on December 30, 2004, with an expiration date of June 28, 2007. On September 21, 2005, DLA granted a separate ATO to support Type Accreditation of the BSM-E, Base Level Support Application (BLSA) Version 1 in accordance with the provisions of DOD 8510.1-M with an expiration date of September 12, 2008 (see Attachment 1-1).
1b. That the Director, DLA, require the CIO/DAA to develop DLA IA policies and guidelines as required by DLA One Book.	Nonconcur	The reason for nonconcurrence with this recommendation is that the CIO/DAA has published the following One Book Chapters to facilitate DLA's implementation of DOD Information Assurance (IA) requirements: • DLA IA Management Controls • DLA IA Operational Controls • DLA IA Technical Controls • DLA IA Rules of Behavior Process • DLA IA Training, Certification, and Workforce Management Requirements included within these One Book Chapters fully address the policies required to implement and sustain an effective IA Program.

Attachment 1

Department of Defense Office of Inspector General (DODOIG) Audit
Review of the Information Security Operational Controls of the Defense Logistics Agency's
Business Systems Modernization-Energy
Comment Matrix on the Recommendations
February 21, 2006

DODIG Recommendations	DLA Response	Remarks/Rationale
1c. That the Director, DLA, require the CIO/DAA to create a management control program that ensures compliance with all DOD and DLA IA policies and guidelines.	Nonconcur	The reason for nonconcurrence with this recommendation is that DLA has an effective IA management control program in place to ensure compliance with IA policies and guidelines. Appropriate IA management control requirements are delineated in the IA Management Control One Book Chapter that establishes responsibility for ensuring IA requirements are enforced by appropriate levels throughout the DLA organization. In addition, IA Performance Reviews are performed on a continuous basis to provide an independent assessment of the IA Program implementation across the Agency. In addition, DLA does not concur with the DODIG draft report findings that indicate DLA is responsible for ensuring Military Service personnel comply with DOD IA requirements (i.e., DLA did not require Military Service users to implement necessary access controls and was unaware of who was accessing BSM-E (FAS) at BSM-E (FAS) user sites.) The BSM-E BLSA Type Accreditation clearly delineates Military Service personnel IA responsibilities (i.e., SSAA, paragraph 4.8.2) and DLA does not have enforcement authority or responsibility for ensuring their compliance (see Attachment 1-2). Additionally, in accordance with DOD 8510.1-M, operational organizations are responsible for ensuring compliance with the provisions and requirements outlined within a Type Accreditation.

Attachment 1

Department of Defense Office of Inspector General (DODOIG) Audit
Review of the Information Security Operational Controls of the Defense Logistics Agency's
Business Systems Modernization-Energy
Comment Matrix on the Recommendations
February 21, 2006

DODIG Recommendations	DLA Response	Remarks/Rationale
1d. That the Director, DLA, develop a DLA plan of action and milestones pertaining to the significant management control weaknesses identified above and continue to report progress on corrective actions to the ASD(NII) on a quarterly basis, beginning March 2006, until all corrective actions are completed and verified as required by FISMA.	Nonconcur	DLA does not believe additional IA management controls are required as indicated in the above responses and therefore nonconcurs with the need to establish a POAM or report on the implementation of controls that are currently in place.
2a. That the CIO/DAA require the Information Operations Directorate, Fort Belvoir (J6F), no later than March 2006, to update the BSM–E POAM to include all security weaknesses based on the current system configuration.	Concur with comments	Joint Interoperability Test Command conducted testing of FAS in 2003. During that test a number of IA remediation actions were identified. When FAS received its Acquisition Decision Memorandum in April 2004, one of the action items was to "Provide monthly report on the status of IA remediation actions to DOT&E and ASD (NII) DCIO-IA." The PMO provided those updates the 15th of each month. The last report was sent in March 2005. At that time, 18 deficiencies were considered fully remediated with 11 still in work in J6F. Corrective actions for the remaining BSM-E BLSA security vulnerabilities have been completed as part of Version 2.0 and are currently undergoing testing. An ATO to support Type Accreditation of Version 2.0 will be granted upon successful completion of this testing.
2b. That the CIO/DAA require the Information Operations Directorate, Fort Belvoir (J6F), no later than March 2006, to create formal procedures for the granting of access and removal of BSM-E Base Level users and Fuels Enterprise Server users at the Base Level.	Concur with comments	The DLA CIO/DAA will direct J6F take actions to implement appropriate measures for granting user access to the Fuels Enterprise Server. However, J6F is not responsible for ensuring implementation of appropriate measures for granting user access to the BSM-E BLSA. Under provisions within the Type Accreditation, this responsibility rests with the respective operational organizations as stipulated in BSM-E BLSA SSAA, paragraph 4.8.2, Hosting Site Responsibilities (see Attachment 1-2).

Attachment 1

Department of Defense Office of Inspector General (DODOIG) Audit
Review of the Information Security Operational Controls of the Defense Logistics Agency's
Business Systems Modernization-Energy
Comment Matrix on the Recommendations
February 21, 2006

DODIG Recommendations	DLA Response	Remarks/Rationale
2c. That the CIO/DAA require the Information Operations Directorate, Fort Belvoir (J6F), no later than March 2006, to create a formal and standard User Agreement/Rules of Behavior document before allowing access to BSM-E.	Nonconcur	The DLA IA Rules of Behavior Process One Book Chapter includes appropriate agreements for different levels of DLA system users (i.e., privileged and non-privileged users). Users of all DLA systems are required to sign this agreement acknowledging receipt and understanding prior to being granted system access. The DLA CIO/DAA will continue to emphasize J6F ensure compliance with the requirements of this One Book Chapter for all Fuels Enterprise Server users. However, DLA is not responsible for ensuring Military Service personnel comply with our DLA policy for granting access to the BSM-E BLSA. In accordance with the BSM-E BLSA Type Accreditation SSAA paragraph 4.8.2, Hosting Site Responsibilities, and DOD 8510.1-M requirements, this responsibility rests with the operational organization (see Attachment 1-2).
2d. That the CIO/DAA require the Information Operations Directorate, Fort Belvoir (J6F), no later than March 2006, to update the BSM-E COOP to correct inconsistencies with the BSM-E SSAA.	Concur with comments	The BSM-E application is currently in the process of transitioning to the DLA Enterprise Data Center (EDC). As a result of this transition, the current BSM-E COOP is being updated for integration into the new DLA EDC computing environment. Finalization of this COOP update and associated testing are contingent upon completion of the BSM-E application migration activities.
2e. That the CIO/DAA require the Information Operations Directorate, Fort Belvoir (J6F), no later than March 2006, to perform a complete test of the COOP for BSM–E.	Concur with comments	The BSM-E application is currently in the process of transitioning to the DLA EDC. As a result of this transition, the current BSM-E COOP is being updated for integration into the new DLA EDC computing environment. Finalization of this COOP update and associated testing are contingent upon completion of the BSM-E application migration activities.

Attachment 1

Department of Defense Office of Inspector General (DODOIG) Audit
Review of the Information Security Operational Controls of the Defense Logistics Agency's
Business Systems Modernization-Energy
Comment Matrix on the Recommendations
February 21, 2006

DODIG Recommendations	DLA Response	Remarks/Rationale
3a. That the Information Operations Directorate, Fort Belvoir (J6F), no later than March 2006, create a MOU/A with the BSM-E Base Level user sites that defines the responsibilities for ensuring a lock-out function is installed on every workstation that runs BSM-E.	Nonconcur	In accordance with the provisions of DOD 8510.1-M, paragraph C3.3.5, for Type Accreditation, DLA has included the appropriate IA operational requirements within the BSM-E BLSA SSAA, paragraph 4.8.2 (see Attachment 1-2). The SSAA supporting Type Accreditation eliminates the need for a separate MOU/A between DLA and BSM-E Base Level user sites. The specific provisions within the BSM-E BLSA SSAA are binding on all organization(s) where this application is installed and operated. Military Service organizations can opt to separately accredit BSM-E BLSA in accordance with DOD 8510.1-M if they choose not to comply with the Type Accreditation requirements.
3b. That the Information Operations Directorate, Fort Belvoir (J6F), no later than March 2006, create a MOU/A with the BSM-E Base Level user sites that defines the responsibilities for evaluating network settings at Base Level sites to ensure that only current users have access to BSM-E.	Nonconcur	In accordance with the provisions of DOD 8510.1-M, paragraph C3.3.5, for Type Accreditation, DLA has included the appropriate IA operational requirements within the BSM-E BLSA SSAA, paragraph 4.8.2 (see Attachment 1-2). The SSAA supporting Type Accreditation eliminates the need for a separate MOU/A between DLA and BSM-E Base Level user sites. The specific provisions within the BSM-E BLSA SSAA are binding on all organization(s) where this application is installed and operated. Military Service organizations can opt to separately accredit BSM-E BLSA in accordance with DOD 8510.1-M if they choose not to comply with the Type Accreditation requirements.

Attachment 1

Department of Defense Office of Inspector General (DODOIG) Audit
Review of the Information Security Operational Controls of the Defense Logistics Agency's
Business Systems Modernization-Energy
Comment Matrix on the Recommendations
February 21, 2006

DODIG Recommendations	DLA Response	Remarks/Rationale
3c. That the Information Operations Directorate, Fort Belvoir (J6F) no later than March 2006 create a MOU/A with the BSM-E Base Level user sites that defines the responsibilities for creating a formal policy for the removal of inactive accounts after 30 days on inactivity.	Nonconcur	In accordance with the provisions of DOD 8510.1-M, paragraph C3.3.5 for Type Accreditation, DLA has included the appropriate IA operational requirements (to include account control) within the BSM-E BLSA SSAA paragraph 4.8.2. The SSAA supporting Type Accreditation eliminates the need for a separate MOU/A between DLA and BSM-E Base Level user sites (see attachment 1-2). The specific provisions within the BSM-E BLSA SSAA are binding on all organization(s) where this application is installed and operated. Military Service organizations can opt to separately accredit BSM-E BLSA in accordance with DOD 8510.1-M if they choose not to comply with the Type Accreditation requirements.
3d. That the Information Operations Directorate, Fort Belvoir (J6F), no later than March 2006, create a MOU/A with the BSM-E Base Level user sites that defines the responsibilities for requiring Base Level to ensure BSM-E backup software is stored at a location separate from the operating location and in an appropriate manner.	Nonconcur	In accordance with the provisions of DOD 8510.1-M, paragraph C3.3.5, for Type Accreditation, DLA has included the appropriate IA operational requirements (to include continuity of operations) within the BSM-E BLSA SSAA, paragraph 4.8.2 (see Attachment 1-2). The SSAA supporting Type Accreditation eliminates the need for a separate MOU/A between DLA and BSM-E Base Level user sites. The specific provisions within the BSM-E BLSA SSAA are binding on all organization(s) where this application is installed and operated. Military Service organizations can opt to separately accredit BSM-E BLSA in accordance with DOD 8510.1-M if they choose not to comply with the Type Accreditation requirements.

Attachment 1

Department of Defense Office of Inspector General (DODOIG) Audit
Review of the Information Security Operational Controls of the Defense Logistics Agency's
Business Systems Modernization-Energy
Comment Matrix on the Recommendations
February 21, 2006

DODIG Recommendations	DLA Response	Remarks/Rationale
3e. That the Information Operations Directorate, Fort Belvoir (J6F), no later than March 2006, create a MOU/A with the BSM-E Base Level user sites that defines the responsibilities for ensuring BSM-E users are provided annual security awareness training consistent with the requirement of DODD 8570.1	Nonconcur	DODI 8500.2, paragraphs 5.7 and 5.7.7, assigns responsibility for "ensuring that IA awareness, training, education, and professionalization are provided to all military and civilian personnel, including contractors, commensurate with their respective responsibilities...." to the DOD Component Head. Military Service personnel at BSM-E Base Level user sites should have received security awareness training as a prerequisite to gaining local area network access. DLA is responsible for and includes training on the application security controls as part of its normal BSM-E BLSA user training.
3f. That the Information Operations Directorate, Fort Belvoir (J6F), no later than March 2006, create a MOU/A with the BSM-E Base Level user sites that defines the responsibilities for tracking users with significant security responsibility and ensure those users are being properly trained consistent with the requirements in DODD 8570.1.	Nonconcur	DODI 8570.1, paragraph 5.9, and DODI 8500.2, paragraphs 5.7 and 5.7.7, assigns responsibility for "ensuring that IA awareness, training, education, and professionalization are provided to all military and civilian personnel, including contractors, commensurate with their respective responsibilities...." to the DOD Component Head. Military Service personnel at BSM-E Base Level user sites should have received security awareness training as a prerequisite to gaining local area network access. DLA is responsible for and includes training on the application security controls as part of its normal BSM-E BLSA user training.
3g. That the Information Operations Directorate, Fort Belvoir (J6F), no later than March 2006, create a MOU/A with the BSM-E Base Level user sites that defines the responsibilities for ensuring backup and recovery procedures exist and are being followed at the BSM-E Base Level	Nonconcur	In accordance with the provisions of DOD 8510.1-M, paragraph C3.3.5 for Type Accreditation, DLA has included the appropriate IA operational requirements (to include Continuity of Operations) within the BSM-E BLSA SSAA, paragraph 4.8.2 (see Attachment 1-2). The SSAA supporting Type Accreditation eliminates the need for a separate MOU/A between DLA and BSM-E Base Level user sites. The specific provisions within the BSM-E BLSA SSAA are binding on all organization(s) where this application is installed and operated. Military Service organizations can opt to separately accredit BSM-E BLSA in accordance with DOD 8510.1-M if they choose not to comply with the Type Accreditation requirements.

Attachment 1

Team Members

The Department of Defense Office of the Deputy Inspector General for Auditing, Readiness and Operations Support prepared this report. Personnel of the Department of Defense Office of Inspector General who contributed to the report are listed below.

Kathryn M. Truex
Sarah A. Davis
Christopher M. Scrabis
Zachary M. Williams